



NEWS RELEASE

F5 Placed in the Leader Tier of the SecureQLab 2026 Cloud WAAP v5.0 CyberRisk Validation Comparative Report

2026-08-03

Independent testing places F5 Distributed Cloud Web App and API Protection in the report's top tier for combined security efficacy and operational efficiency

SEATTLE--(BUSINESS WIRE)-- F5 (NASDAQ: FFIV), the global leader in delivering and securing every app and API, announced that **F5 Distributed Cloud Web App and API Protection (WAAP)**, part of the **F5 Application Delivery and Security Platform (ADSP)**, was placed in the Leader tier of SecureQLab's 2026 Cloud WAAP v5.0 CyberRisk Validation Comparative Report. F5 was one of a select few evaluated vendors to earn both the Secure-by-Design and Secure-by-Default certifications.

F5 in the Leader tier of the SecureQLab Cloud WAAP v5.0 CyberRisk Validation Comparative Report.

Enterprises buying application security products have long faced a trade-off. Some solutions

stop sophisticated attacks but demand constant tuning and specialized staff to run. Others deploy easily but leave gaps that only surface after a breach. Security teams end up choosing which problem they would rather have.

The SecureQLab evaluation measured both sides of the efficiency/efficacy trade-off. F5 was placed in the Leader tier of the CyberRisk Ripple—the report's highest classification, reserved for solutions scoring in the top tier for protection and operations. F5 scored 92.7% Security Efficacy and 94.7% Operational Efficiency, exceeding the

measured group averages of 86.8% and 93.8%, respectively.

“Frontier AI has made traditional security approaches untenable, compressing or inverting the time between vulnerability disclosure and working exploit,” said John Maddison, Chief Marketing Officer at F5. “Enterprises are protecting more applications, more APIs, and now more AI—and security that only works when you staff a skilled team around it isn’t security that scales.”

Today’s enterprises need a WAAP solution with virtual patching tools such as web application firewall (WAF) capabilities in front of the application—blocking exploitation on day one, without new signatures and without constant tuning. At the same time, modern organizations can’t afford to take any single vendor’s word for how well their solutions work. Security leaders benefit from independent testing to verify which tools sufficiently provide advertised protections.

Protection that holds up under test conditions

SecureIQLab subjected each solution to more than 1,600 attack scenarios spanning OWASP web application attacks, API attacks, bot and AI-assisted bot attacks, Layer 7 DoS and DDoS, security resiliency, and a WAAP vulnerability assessment, with legitimate traffic running throughout to measure false positive avoidance. Testing was AMTSO-compliant (Testing Protocol Standard v1.3) under AMTSO Test ID AMTSO-LS1-TP169 and executed on SOCx[®], SecureIQLab’s AI-Driven Cloud Security Validation Platform, to ensure consistent execution across vendors.

Operations without the drag

F5’s 94.7% Operational Efficiency score reflects an architecture designed to reduce work rather than create it. F5 Distributed Cloud WAAP fuses WAF, API security, bot defense, and Layer 3–4 and 7 DDoS mitigation into a single-pass inspection architecture, so traffic is decrypted and evaluated once rather than passing between loosely integrated products for inspection and enforcement. Platform teams can deploy and scale policy without stacking latency or configuration overhead, and the same battle-tested WAF engine runs across F5 Distributed Cloud Services, F5 BIG-IP Advanced WAF, and F5 NGINX solutions.

Security built in, not bolted on

The Secure-by-Design and Secure-by-Default certifications are awarded to solutions that do not expand the attack surface of the environments they protect and that deliver meaningful protection without additional configuration. Earning both requires a score above 85% in each category and a perfect 100% on the WAAP vulnerability assessment. F5 was one of five solutions to clear that bar.

F5 also scored above the group average on compliance, a category assessing how effectively a solution supports regulatory, data protection, audit, and governance requirements drawn from frameworks including NIST SP 800-53, the NIST AI Risk Management Framework, ISO/IEC 27001, ISO/IEC 42001, PCI DSS, GDPR, HIPAA, and SOC 2. In addition, F5 scored 100% on the OWASP LLM Top 10 subset in scope for v5.0, which covers two risk categories: Prompt Injection (LLM01:2025) and Improper Output Handling (LLM05:2025). Testing also included 35 benign test cases to measure false positives.

“The cloud WAAP market has matured significantly. The group average security score rose roughly 12.3% over the previous edition of this test, and for the first time we scored AI application security as its own category, because that is where the attack surface is expanding,” said David Ellis, VP of Research, SecureQLab. “Solutions placed in the Leader tier demonstrated coverage across web application, API, advanced threat, and AI-enabled application attacks.”

Supporting materials

- Resource: [SecureQLab Cloud WAAP v5.0 CyberRisk Validation Comparative Report](#)
- Blog: [SecureQLab’s independent multi-vendor testing puts F5 in the Leader tier for security and operational efficiency](#)
- Solution page: [F5 web application and API protection](#)

About the SecureQLab evaluation

SecureQLab tested the products named in the Cloud WAAP v5.0 CyberRisk Validation Comparative Report on the dates listed in the report methodology section. SecureQLab does not endorse, certify, warrant, or guarantee the performance or safety of any tested product. Test results reflect performance under the specific methodology and scenarios in that section only. The findings referenced in this release apply to the specific product versions, deployment configurations, and test scenarios listed in the report. Performance under other versions, configurations, or scenarios is not implied. Past performance is not a forecast of future results.

About F5

F5, Inc. (NASDAQ: FFIV) is the global leader that delivers and secures every app. Backed by three decades of expertise, F5 has built the industry’s premier platform—F5 Application Delivery and Security Platform (ADSP)—to deliver and secure every app, every API, anywhere: on-premises, in the cloud, at the edge, and across hybrid, multicloud environments. F5 is committed to innovating and partnering with the world’s largest and most advanced organizations to deliver fast, available, and secure digital experiences. Together, we help each other thrive and bring a better digital world to life.

For more information visit **f5.com**

Explore F5 Labs threat research at **f5.com/labs**

Follow to learn more about F5, our partners, and technologies: **Blog** | **LinkedIn** | **X** | **YouTube** | **Instagram** | **Facebook**

F5, BIG-IP, Advanced WAF, and NGINX are trademarks, service marks, or tradenames of F5, Inc. or its affiliates in the U.S. and other countries. All other product and company names herein may be trademarks of their respective owners. The validation described herein does not create a partnership, joint venture, agency relationship, or endorsement between the parties.

Source: F5, Inc.

Dan Sorensen

F5

(650) 228-4842

d.sorensen@f5.com

Holly Lancaster

We. Communications

(415) 547-7054

hlancaster@wecomcommunications.com

Source: F5, Inc.